October 31st 2022

Sybil Defense Report

In Favor of the Quadratic Funding

Prepared and submitted by: Gray Egboluche
Data Scientist

Sybil Attacks

In a Sybil assault, the attacker generates a large number of pseudonymous identities and uses them to exert disproportionate influence on a network service's reputation system. It is named after Sybil, a case study of a woman diagnosed with dissociative identity disorder and the subject of the book Sybil.

Due to the quadratic funding system's inherent tendency to prioritize the number of funders over the amount of funded, it is vulnerable to sybil attacks.

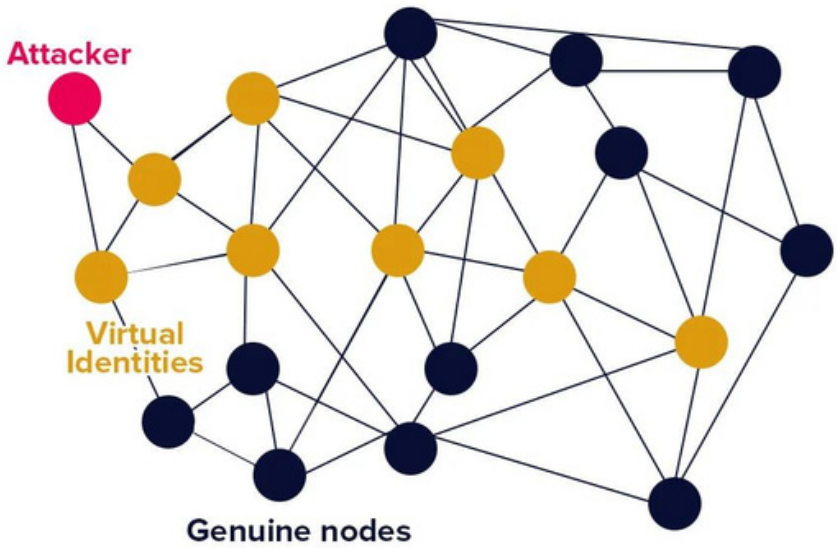
Objectives

My objective for taking part in this hackathon is to implement a long-lasting defense against sybil attacks, maintaining the credibility of the quadratic system.

Common Sybil Traits

Due to their inability to replicate actual user activity, Sybils have a certain behavioral pattern.
Listed below are a few behavioral trends.:

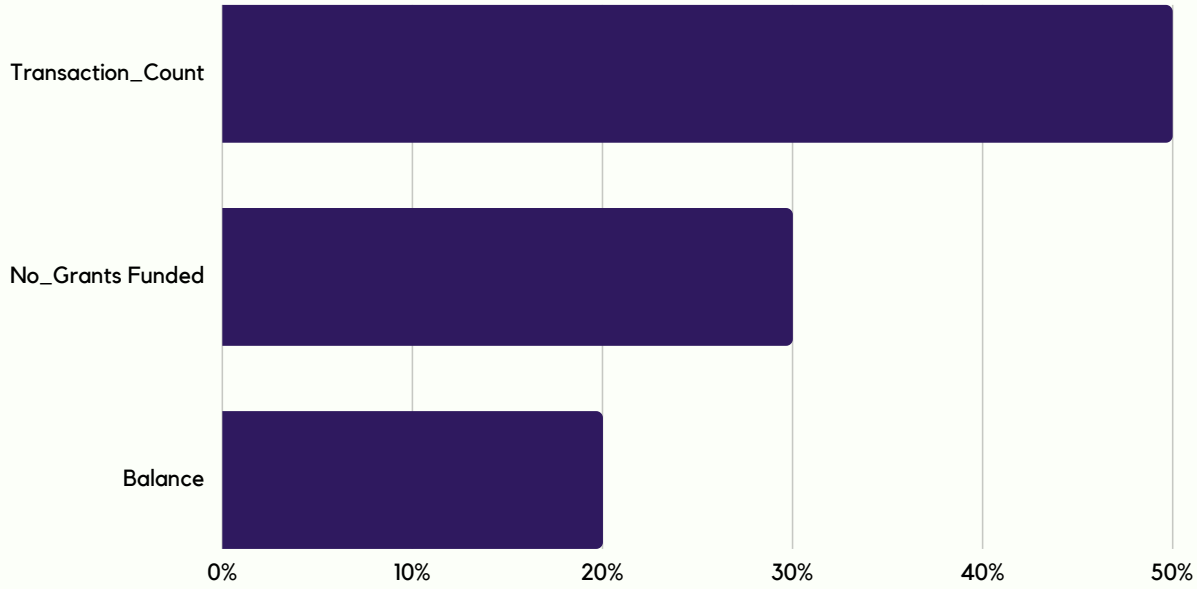
- Obtain funds from the same bridge.
- Donate only to one grant.
- Stop all activity once nonce 5 is reached or before.
- Low Ethereum balance
- Rarely have any activity on the Ethereum blockchain



Source: Swathi, Modi, & Patel, 2019

Key Sybil Indicators

The number of transactions, Grants funded, and Balance are all reasonable grounds for suspecting sybil activity



The balance, transaction count, and grants funded are the three most important indicators, and they are arranged according to significance. Grants funded and balance are at 30% and 20%, respectively, while the transaction count is at 50%. While other indications are essential, transaction count seems to be the most dependable of them all.

Transaction count is assigned a larger percentage owing to the consistency; to create several identities with a decent number of transactions would not only be time consuming but also cost more money.

The quantity of grants funded is another reliable signal because it's quite improbable that a sybil attacker would fund many donations, negating the attack's intent. However, there is a strong probability that a real donor will only support one grant; as a result, a 30% scoring power is given.

Point System

Introducing the Point System.
The solution we have been looding for ?

The point system, which assigns points to users who reach certain degrees of activity, is a method that categorizes users based on their on-chain behavior. Currently, it employs the three primary Sybil indicators (balance, transaction count, and number of Grants funded), with varying weights given to each criterion.

Determining Points Threshold

Transaction count - To allow for funds with new addresses without being tagged as sybils, the class limitations for transaction counts were changed to range between the 25th percentile (9 transactions). However, active addresses should continue to accumulate appropriate points.

Grants Funded - The number of grants supported reveals a lot about the funder's intentions; financing many grants will assist to mitigate the effect of the Sybil assault. Although it is quite likely that only one grant will be funded, this will not disrupt the system.

Balance - Because of its unstable nature, the balance was assigned the lowest power %; its minimum level fluctuates between (0.000547,0.004721 and >0.004721).

Points and their Categories

Exploring the Categories

An address may fall into one of the non-Sybil, reviewing, or sybil categories, depending on the score it has received.

Sybils -These addresses have been classed as sybils by the point system due to their low point totals; the point range for sybils is any digit below 5.5.

Reviewing -These are addresses that the system is unsure about and unable to categorize as sybils or non-sybils; such addresses are either submitted to be examined by humans or a backup mechanism is in place. The point range for sybils is any digit between 5.5 and 6.5.

Non-Sybils - These are our target audiences—individuals who make it past the point system's screening and are completely accepted as valid funders. points acquired start at values over 6.6.